IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

A.M. CASTLE & CO.,	§	
	§	
Plaintiff,	§	
	§	
VS.	§	Civ. A. H-13-2960
	§	
THOMAS K. BYRNE AND OILFIELD STEEL SUPPLY, LLC,	§	
	§	
Defendants.	§	

OPINION AND ORDER

Pending before the Court in the above referenced cause, alleging breach of employee confidentiality agreement, breach of fiduciary duty, unjust enrichment, tortious interference with contract, tortious interference with prospective economic advantage, and civil conspiracy, and seeking compensatory and injunctive relief against a former employee of Plaintiff A.M. Castle & Co. ("Castle"), Thomas K. Byrne ("Byrne"), and his new employer, Oilfield Steel Supply, LLC ("OSS")(collectively "Defendants"), are Castle's objections (instrument #53) to United States Magistrate Judge Frances Stacy's order (#52) granting in part and denying in part Defendants' motion to compel (#42) and denying Castle's motion to compel and request for show cause order (#44).

Castle and OSS are direct competitors in supplying pipe and materials to the oil and gas industry. Byrne was employed initially by Tube Supply, Inc., which was acquired by Castle, a

Maryland corporation with its principal place of business in Illinois, as an Inside Sales Representative in Houston, Texas. By virtue of his employment in Castle's Oil & Gas business unit, Castle claims that Byrne had access to its confidential information. Byrne signed a confidentiality agreement in April 2009 when Tube Supply was his employer, promising not to use his employer's confidential information for the benefit of any third parties. Byrne resigned from Castle on April 30, 2013 and went to work for OSS. Castle claims that over a course of months before he resigned, Byrne misappropriated confidential information, including customer lists and information, vendor contact information, and sales and revenue data, and subsequently provided them to his new employer, OSS. Furthermore, according to Castle, Byrne then began soliciting Castle's customer and vendor lists on behalf of OSS from this wrongfully obtained information.

In its objections to the Magistrate Judge Stacy's rulings on Castle's motions to compel, Castle contends that Defendants did not perform a thorough search of all computers and electronic devices potentially having relevant information and therefore ask the Court to give it physical access to Defendants' electronic devices.

Standard of Review

This Court referred the motions to compel to United States Magistrate Judge Frances Stacy under 28 U.S.C. section 636(b)(1)(A) for resolution.

A magistrate judge is permitted broad discretion in resolving nondispositive pretrial motions. *Id.* A magistrate's order for nondispositive matters may only be reconsidered where it has been shown that the magistrate judge's order is clearly erroneous or contrary to law. *Id.*; Fed. R. Civ. P. 72(a)[1]; *Moore v. Ford Motor Co.*, 755 F.3d 802, 806 & n.6 (5th Cir. 2014). Thus factual findings are reviewed under a clearly erroneous standard and legal conclusions are reviewed *de novo*. *Moore*, 755 F.3e at 806 & n.7, *citing Alldread v. City of Granada*, 988 F.2d 1425, 1434 (5th Cir. 1993).

Relevant Discovery Rules

Under Federal Rule of Civil Procedure 26(b)(1), "Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense." Moreover, "[r]elevant information need not be admissible at trial if the discovery appears reasonably calculated to lead to discovery of admissible

---

[1] Rule 72(a), "Nondispositive Matters, provides,

> When a pretrial matter not dispositive of a party's claim or defense is referred to a magistrate judge to hear and decide, the magistrate judge must promptly conduct the required proceedings and, when appropriate, issue a written order stating the decision. A party may serve and file objections to the order within 14 days after being served with a copy. A party may not assign as error a defect in the order not timely objected to. The district judge in the case must consider timely objections and modify or set aside any part of the order that is clearly erroneous or contrary to law.

evidence." *Id.* "Relevant evidence" is "evidence having any tendency to make the existence of any fact more probable or less probable than it would be without the evidence." Fed. R. Evid. 401.

In 2006 Federal Rule of Civil Procedure 34 was amended to allow a party to explicitly request production of electronically stored information just as it had been allowed to seek production of paper documents.[2] Federal Rule of Civil Procedure 34 provides

---

[2] Rule 34 provides in relevant part,

> (a) **In General.** A party may serve on any other party a request within the scope of Rule 26(b):
>
> (1) to produce and permit the requesting party or its representative to inspect, copy, test or sample the following items in the responding party's possession, custody, or control:
>
> > (A) any designated documents or electronically stored information-including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data-stored in any medium from which information can be obtained either directly, or if necessary, after translation by the responding party into a reasonably usable form; or
> >
> > (B) any designated tangible things; or
>
> (2) to permit entry onto designated land or other property possesses or controlled by the responding party, so the requesting party may inspect, measure, survey, photograph, test or sample the property or any designated object or operation on it.
>
> (b) Procedure
>
> (1) *Contents of the Request.* The request:
>
> > (A) must describe with reasonable particularity

that a party may request another party to produce "electronically stored information . . . stored in any medium from which information can be obtained"[3] and requires that a document request "must describe with reasonable particularity each item or category of items to be inspected" or produced.

The party receiving the request "must respond in writing within 30 days after being served" [Rule 34(b)(2)(A)] and "[f]or each item or category, the response must either state that the inspection . . . will be permitted as requested or state an objection to the request, including the reasons [Rule 34(b)(2)(B)]." When a request for production or an interrogatory is not answered, the party seeking discovery may move for an order compelling production against the nonresponding party under Federal Rule of Civil Procedure 37(a)(3). An evasive or incomplete answer

---

> each item or category of items to be inspected;
>
> (B) must specify a reasonable time, place, and manner for the inspection and for performing the related acts; and
>
> (C) may specify the form or forms in which electronically stored information is to be produced.

[3] The Advisory Committee notes to the 2006 amendment state, "Rule 34(a) is amended to confirm that the discovery of electronically stored information stands on equal footing with the discovery of paper documents. . . . [A] Rule 34 request for production of 'documents' should be understood to encompass, and the response should include, electronically stored information unless discovery in the action has clearly distinguished between electronically stored information and 'documents.'"

is deemed to be a failure to respond. Fed. R. Civ. P. 37(a)(4).

Federal Rule of Civil Procedure 26(b)(2)(B) permits the district court to compel production of information that is not reasonably available only "if the requesting party shows good cause."[4] To determine if the party has shown "good cause," among factors that the court should consider are whether "the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of discovery in resolving the issues." Rule 26(b)(2)(C)(iii).

Because granting a party access to an opponent's electronic storage device, itself, is highly intrusive, according to the Advisory Committee's comments to the 2006 amendments to Rule 34, while direct "access [to a party's electronic storage device] might be justified in some circumstances," the rules were "not meant to

---

[4] Rule 26(b)(2)(B)("*Specific Limitations on Electronically Stored Information*") provides,

> A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C).

create a routine right of direct access" and court should "guard against undue intrusiveness." Thus courts are very cautious about ordering mirror imaging of computers, especially where the request is overly broad and where the connection between the party's claims and the computer is vague and unproven. *See, e.g., Han v. Futurewei Technologies, Inc.*, No. 11-CV-831-JM(JMA), 2011 WL 4344301 (S.D. Cal. Sept. 15, 2011)(denying Defendant Huawei Technologies' request for an order requiring Plaintiff Jun Han to allow Defendant to copy the hard drives of her personal computing device (1) because the discovery she sought "bears no relevance to the claims and defenses presently in the case," (2) because Defendant failed to show that Plaintiff Han was in wrongful possession of any company documents or to provide an expert declaration or other evidence that Plaintiff was copying, removing, deleting or wiping files off the computer, and (3) because serving discovery requests (interrogatories or document requests) for the information was a more convenient, less burdensome and less expensive way to obtain the information), citing *In re Weekley Homes, LP*, 295 S.W. 3d 309, 317 (Tex. 2009)(opining that under federal case law, direct access to a party's electronic device requires a showing by the requesting party that the responding party has "defaulted in its obligation to search its records and produce the requested data."), and *Balfour Beatty Rail, Inc. v. Vaccarello*, Case No. 3:06-cv-551-J-20MCR, 2007 WL 169628, at *3

(M.D. Fla. Jan. 18, 2007)(denying access to responding party's computer hard drives when requesting party did not show what it was seeking to discover from them or to establish that the responding party failed to comply with discovery obligations). Courts are more willing to require production where the electronic discovery sought is relevant to the claims and defenses in the suit. *See e.g., Ameriwood Indus. Inc. v. Liberman*, No. 4:06CV534-DJS, 2006 WL 3825291, at *1 (E.D. Mo. Dec. 27, 2006)(where plaintiff's former employees were sued by plaintiff for improperly using plaintiff's computers, confidential files, and confidential information to sabotage plaintiff's business and to divert plaintiff's business to themselves, the court found that the close relationship between plaintiff's claims and defendants' computer equipment and the evidence raised questions whether defendants had produced all responsive documents and allowed an independent expert to obtain and search a mirror image of defendants' computer equipment); *Genworth Fin. Wealth Mgmt., Inc. v. McMullan*, 267 F.R.D. 443, 447-48 (D. Conn. 2010)(finding sufficient nexus between claims and need for computer imaging where plaintiff alleged that defendant used the computers to disseminate plaintiff's confidential information); *Frees, Inc. v. McMillian*, Civ. A. No. 05-1979, 2007 WL 184889, at *2 (W.D. La. Jan 22, 2007)(permitting imaging of defendant's computer where plaintiff alleged that defendant had stolen plaintiff's proprietary computer files) *aff'd*, 2007 WL 13088388

(W.D. La. 2007); *Jacobson v. Starbucks Coffee Co.*, 2006 WL 3146349, at *8 (D. Kan. Oct. 31, 2005)(Although noting that "production of a computer for inspection is unusual," finding that the record "reflects a history of incomplete and inconsistent responses to plaintiff's production requests" regarding which "the computer has relevant information" and thus compelling its production or a mirror image). *Cf. Balboa Threadworks, Inc. v. Stucky*, 2006 WL 763668, at *3 (D. Kan. 2006)("Courts have been cautious in requiring the mirror imaging of computers where the request is extremely broad in nature and the connection between the computers and the claims in the lawsuit are unduly vague or unsubstantiated in nature."); *McCurdy Group v. American Biomedical Group, Inc.*, 9 Fed. Appx. 822, 831 (10th Cir. 2009)(affirming the district court's denial of a request to compel production of the opponent's computer hard drives as a "drastic discovery measure" in light of the movant's failure to explain why it should be allowed to inspect them and its only assertion was that it was skeptical that the opponent had produced copies of all relevant and nonprivileged documents from the hard drives).

Given the concerns about intrusiveness and privacy, one area where courts have allowed a requesting party to obtain a mirror image[5] of a producing party's computer is where the computer was

[5] *See U.S. v. Triumph Capital Group, Inc.* 211 F.R.D. 31, 48 (D. Conn. 2002)("A mirror image is an exact duplicate of the entire hard drive, and includes all the scattered clusters of the

used to download trade secrets, the misappropriation of which is the suit's issue. *See, e.g., Weatherford U.S. LP v. Innis*, No. 4:09-CV-061, 2011 WL 2174045, at *4 (D.N.D. June 2, 2011), *citing Balboa*, 2006 WL 763668 at *3; *Ameriwood Indus.*, 2006 WL 3825291, at *2-3. Where there are discrepancies or inconsistencies in the responding party's discovery responses, a court may allow an expert to examine a mirror image of the party's hard drives. *Ameriwood Indus.*, 2006 WL 3825291, at *4, *citing Simon Prop. Group, LP v. mySimon, Inc.*, 194 F.R.D. 639, 641 (S.D. Ind. 2000)(permitting plaintiff to review the mirror image of defendant's computers where there were "troubling discrepancies with respect to defendant's document production").

To establish a cause of action for misappropriation of trade secrets under Texas common law, Castle must show that (1) a trade secret existed, (2) that Defendants acquired the trade secret through improper means, and (3) that they disclosed the trade secret without Castle's consent. *Wellogix, Inc. v. Accenture, LLP*, 716 F.3d 867, 874 (5th Cir. 2013); Texas Uniform Trade Secrets Act ("TUTSA"), Tex. Civ. Prac. & Rem. Code section 134A.002.[6] A trade

---

active and deleted files and the slack and free space."); *Balboa Threadworks, Inc. v. Stucky*, 2006 WL 763668, at *3 (D. Kan. 2006)(A "mirror image" is "a forensic duplicate, which replicates bit for bit, sector for sector, all allocated and unallocated space, including slack space, on a computer hard drive.").

[6] TUTSA specifically states that "Except as provided by Subsection (b), this chapter displaces conflicting tort . . . law of this state providing civil remedies for misappropriation of a

secret may consist of

> any formula, pattern device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a patter for a machine or other device, or a list of customers.

4 *Restatement of Torts* sec. 757, Comment b (1939), *cited with approval*, *Hyde Corp. v. Huffines*, 158 Tex. 566, 314 S.W. 2d 763, 776 (1958). Texas requires that a trade secret be "secret", i.e., that it be neither generally known by others in the same business nor readily ascertainable by an independent investigation. *Zoecon Indus. v. Am. Stockman Tag Co.*, 713 F.2d 1174, 1179 (5th Cir. 1983). *See also Carson Products Co. v. Califano*, 594 F.2d 453, 461 (5th Cir. 1979)(However strong other indica of trade secret status is, it must only be acquirable by use of improper means.). The Official Comment to the Restatement (Third) of Torts section 757, Comment (b) at 5, provides criteria for determining whether something is a trade secret:

> An exact definition of a trade secret is not possible. Some factors to be considered in determining whether given information is one's trade secret are: (1) The extent to which the information is known outside his business; (2) The extent to which it is known by employees and others involved in his business; (3) The

---

trade secret." Tex. Civ. Prac. & Rem. Code section 134A.007. Subsection (b)(1) states that "[t]his chapter does not affect . . . contractual remedies, whether or not based upon misappropriation of a trade secret." Therefore Castle's breach of confidentiality agreement claim continues even if its misappropriation of trade secret does not.

> extent of measures taken by him to guard the secrecy of the information; (4) The value of the information to him or his competitors; (5) The amount of effort or money expended by him in developing the information; (6) The ease or difficulty with which the information could be properly acquired or duplicated by others.

The owner of the trade secret does not have to satisfy all six factors because trade secrets do not fit neatly into all factors every time, *General Univ. Sys.*, 379 F.3d at 150, *citing In re Bass*, 113 S.W. 3d 735, 739-40 (Tex. 2003).

Because of the secrecy requirement, the owner of a trade secret must take measures to prevent it from becoming known to persons other than those permitted by the owner to have access for limited purposes. The existence of a trade secret is a question of fact to be decided by the judge or the jury as factfinder. *General Univ. Systems, Inc. v. Lee*, 379 F.3d 131, 150 (5th Cir. 2004), *citing* Restatement (Third) Unfair Competition sec. 39 cmt. (1995). Items such as customer lists, pricing information, client information, customer preferences, and buyer contacts may be trade secrets if they meet the criteria for such. *Global Water Group, Inc. v. Atchley*, 244 S.W. 3d 924, 928 (Tex. App.--Dallas 2008, pet. denied), *citing T-N-Y Motorsports, Inc. v. Hennessey Motorsports, Inc.*, 965 S.W. 2d 18, 22 (Tex. App.--Houston [1st Dist.] 1998, no pet.). *See, e.g., Guy Carpenter & Co. v. Provenzale*, 334 F.3d 459, 467 (5th Cir. 2003)(holding that a customer list may be a trade secret if it is secret and the court examines if it satisfies three factors: "(1) what steps, if any, an employer has taken to

maintain the confidentiality of a customer list; (2) whether a departing employee acknowledges that the customer list is confidential; and (3) whether the content of the list is readily ascertainable.").

Background

United States Magistrate Judge Stacy has issued two orders (#41, on February 13, 2014; and #52, on September 12, 2014) regarding Castle's continuing effort to obtain access to and inspect all computer equipment and electronic devices in the custody or control of Defendants in order to discover "confidential information" allegedly misappropriated from Castle by Byrne.

The first order (#41) denied Castle's request to examine Defendants' electronic devices because it was overly broad and because Castle, in light of the discovery that had been produced by Defendants, had not shown that Defendants defaulted on their discovery obligations. Furthermore the Magistrate Judge opined that "Defendants should be required to search any electronic device used by any former employee or independent contractor of Plaintiff who is now employed by Defendant OSS, for any documents that may belong to Plaintiff." #41 at p. 2. She instructed the parties to discuss their differences and agree on a protocol for Defendants to search their devices and identify any documents on these electronic devices that might belong to Castle and to provide a written report and/or affidavit to Castle.

On March 6, 2014 Defendants sent a letter report (#44-6) to Castle stating that an independent search by Chorus Consulting LLC through CloudNine Discovery[7] ("Chorus") had found no other documents to produce. Castle objected that Defendants had not searched all of the devices and equipment used by all Castle ex-employees who went to work for OSS, including some to whom Byrne had sent emails before Byrne resigned from Castle and who had produced Castle's confidential information when they were subpoenaed by Castle. Castle also claimed that Defendants did not search the OSS e-mail server, which Defendants had identified in their Rule 26(a)(1) initial disclosures as potentially containing responsive information. Moreover, Defendants, despite their denial of having any more information, did subsequently produce 148 new documents that had not been produced previously. #44-8. Castle also argues that Defendants did not provide any information on those devices and drives that they did search, specifically about whether any files had been copied or deleted. Castle asked the Court to order Defendants to submit to a court-supervised forensic

[7] The letter report indicates that Chorus "created forensic images of each device utilizing accepted industry practices," that the original devices were then either quarantined in Chorus' offices or returned to the appropriate custodian," that they were searched for "files that might exist or have existed on these devices arising out of [these individuals'] prior employment or association with Castle or Tube Supply," that the resulting 10,000 plus emails and two files were produced to Castle, and that none of the forensic images and quarantined devices were accessible to Byrne or OSS. #44-6, pp. 2-3.

inspection of Defendants' computers and electronic equipment because of these deficiencies in Defendants' own searches, which Castle claims failed to comply with Magistrate Judge Stacy's orders. *See, e.g., Audio Visual Innovations, Inc. v. Burgdolf*, No. 13-10372, 2014 WL 505565, at *2 (E.D. Mich. 2014)("In situations where a party can show improper conduct on the part of the responding party, a forensic examination may be appropriate.")(ordering forensic imaging of defendant's work and personal computers, external hard drives, and iPhone in a trade secrets and misappropriation case brought by an employer against a former employee).

In the Magistrate Judge's second order of September 12, 2014 (#52), addressing Castle's request for a show cause order, and, again, for an order allowing Castle to inspect Defendants' electronic devices, and Defendants' motion to compel complete responses to specified interrogatories and production requests, Magistrate Judge Stacy granted in part Defendants' requests for supplemental information, but limited it to information "related solely to Plaintiff's 'oil and gas business unit,' where Thomas K. Byrne was employed." She also denied Castle's show cause order request, she found that Defendants had produced information to Castle on numerous occasions, had searched their computers and

electronic storage devices for 288 terms[8] identified by Castle and had given a report of that search to Castle, and that nothing had changed since her previous order that could convince her to order an inspection of Defendants' computers and electronic storage devices. #52 at p. 2.

Castle's Objections (#53)

Because the Court finds that some of Castle's representations about the contents of the evidence attached to #44 are not accurate or are taken out of context, the Court has modified or supplemented some of Castle's quotations to reflect what the documents actually state. It should also be noted that the June 20, 2012 letter from Byrne's counsel to Castle's attorney shortly after the litigation began, quoted by Castle below, reflects that counsel's own review of Byrne's personal laptop and the laptop issued to Byrne by OSS, as well as Byrne's iPhone, was far from complete, so counsel's statements are tentative and contingent on what discovery might reveal since he did not yet know what would be found on the hard drives.

---

[8] The "288" appears to be a typographical error because the letter report indicating compliance with the February 23, 2014 order states that Castle provided a list of 388 search terms, which were searched and which identified 54,785 files, which were then searched for those terms. The resulting 148 data files were then produced to Castle. See #44-8.

In their response (#57 at pp. 4-6 and n.1) to Castle's objections, Defendants, also asserting a typographical error, state that the correct number of such terms was 378, all of which it searched for as detailed in its letter report of July 23, 2014 (#44-8).

Observing that in response to Castle's cease and desist letter, Byrne's counsel, asserting that "we intend to continue our cooperative stance," initially stated that before Byrne's resignation from Castle, "some" of the e-mails he sent from his Castle e-mail account to his home account were "entirely of a personal nature" and one included a "detailed report on fracking provided to Mr. Byrne by a customer, which he sent home intending to review later." #44-1. Counsel acknowledged that Byrne "sent some information to his personal account containing Castle customer contact information and later forwarded those emails to his OSS e-mail account." *Id.* Byrne also sent sales reports, including some "provided to him automatically from Castle detailing his daily sales so that he could keep track of his generation of commission based compensation," and that "these reports may contain sales data about other salespeople as well as his own." *Id.* He represents that Byrne "has contacted some of the customers whose contact information he e-mailed to himself since his employment with OSS. Mr. Byrne may have provided the contact information he e-mailed to his assistant at OSS for Mr. Byrne's own use. Mr. Byrne has not disseminated any of this information to any other person or entity." *Id.* The letter concludes, "[W]e believe that none of this information at issue is confidential. In particular, the contact information that Mr. Byrne emailed himself is information that he could have (and frankly should have) simply reconstructed via

Google searches and other publicly available means after leaving Castle."

Similarly, in a letter from counsel for OSS, counsel also maintained that the e-mail addresses of Byrne's contacts, found on his OSS-issued computer, "are publically available and are certainly not confidential information of Castle." #44-2.

Castle contends that Byrne sent Castle copies of documents that Byrne had in his possession, including reports "clearly marked 'Confidential,' lists of open transactions with Castle's customers, lists identifying the volume of business Castle has transacted with certain customers, lists identifying the largest customers Defendant Byrne serviced while employed at Castle, and contact information for roughly fifty of Castle's customers and vendors." #53 at pp. 2-3. After this lawsuit was filed and written discovery requests were served, Defendants again denied that OSS had confidential information belonging to Castle, and OSS responded that it had no information and no documents regarding work performed by Byrne when he was employed by Castle. Castle then sent out subpoenas to four of its ex-employees who had been interacting with Byrne on OSS-related business before Byrne resigned and who purportedly possessed Castle's information: Nick Jones, Humberto Leniek, Chad Williams, and Corbin Redd. Castle claims that after the Honorable Nancy F. Atlas ordered enforcement of the subpoenas, these four men produced tens of thousands of

pages of Castle's confidential information. #53 at p. 3. Castle contends that from the beginning of this litigation, Defendants have tried to hide the extent of Byrne's misconduct by misrepresenting what information Byrne took and what other information Defendants possessed. After Castle moved to compel forensic discovery (#33), Castle claims that Defendants misrepresented that they had searched all their electronic devices and had produced everything to Castle. Castle asks the Court to authorize an independent inspection of Defendants' devices to find out what Defendants possessed and what they deleted–-"as this is otherwise the classic case of allowing the fox to guard the henhouse door." #53, p. 4, n.1.

Castle charges that Magistrate Judge Stacy erred in failing to enforce the terms of her February 13, 2014 order (#41). Defendants limited their search to exclude the OSS e-mail server and OSS equipment used by ex-Castle employees Nick Jones, Chad Williams and Corbin Redd, even though there was evidence that Byrne had been communicating with these individuals via e-mail before Byrne resigned from Castle and despite evidence that each had confidential Castle information in his possession while employed by OSS. #44-9. Moreover the Magistrate Judge's September 12, 2014 order does not explain why she failed to enforce the prior order regarding the scope of the search ("any electronic device used by any former employee or independent contractor of Plaintiff who is

now employed by Defendant OSS, for any documents that may belong to Plaintiff" [#41 at p.2.]).

Castle asks the Court to vacate the Magistrate Judge's order denying Castle's motion to compel and request for a show cause order because Defendants failed to comply with the Court's February 13, 2014 order. Although on September 9, 2013 Defendants responded to discovery requests that OSS had no documents regarding work performed by Byrne for OSS before he resigned from Castle (#44, Ex. C, par. 4), three weeks later Defendants produced such documents showing that Byrne had performed such work (#44-9, Byrne provided OSS employees Chad Williams, Humberto Leniek, and OSS CEO Nick Jones with specifications for materials that OSS- and ex-Castle-employee Chad Williams intended to order from Tenaris, a Castle supplier). Castle insists that in response to Castle's request for production (#44-3 and -4), it is entitled to know if that transaction was completed and its result.[9] Castle objects to Defendants' pattern of first stating they have produced everything they have in response to Castle's discovery request and then

[9] Defendants point out that the Request for production No. 4 was not the subject of Plaintiff's first motion to compel nor of Magistrate Judge Stacy's February order, both of which dealt with the return to Castle of information that Castle had produced, and which Defendants promised to, and did, return. Defendants maintain that Castle is now trying to expand the February order to cover any document regardless of the objections to discovery requests that Defendants had previously raised, as well as to obtain an completely different subset of discovery requests not raised in Castle's previous motions and which the Magistrate Judge was not asked to consider.

subsequently turning around and producing more documents when compelled to do so by the Court. Castle again complains of Defendants' failure to search the OSS e-mail server, OSS computers and equipment issued to OSS CEO Nick Jones and OSS employees and ex-Castle-employees Humberto Leniek, Chad Williams, and Corbin Redd, and of their failure to provide information about deleted files. Finally Castle again asserts that Magistrate Judge Stacy erred in denying Castle's request for a court-managed forensic examination of OSS's computers that will reveal Castle's confidential information possessed now or at one time by Defendants, where that information was stored, whether it was copied or transferred elsewhere, who had access to it, and how it has been used.

Castle also objects to Magistrate Judge Stacy's September 12, 2014 order because it allowed discovery of so much irrelevant information in Castle's records about its employees, e.g., separation dates and reasons for termination, names of all employees who had access to the proprietary and confidential information that Defendants allegedly took from Castle, and information relating to customer issues or losses.

Defendants' Response (#57)

In response, Defendants point out that in her September Order, Judge Stacy ruled that Defendants had complied with her February order and Plaintiffs failed to meet the high burden of proof to be

entitled to conduct its own forensic examination of Defendants' electronic devices; since the Magistrate Judge authored the February order, they urge that she is in the best position to interpret it. Moreover they argue that because the order was not clearly erroneous, Castle's objection should be overruled.

Defendants also contend that the Magistrate Judge did not err in granting their motion to compel additional information because Castle had failed to produce documents supporting its allegations of tortious interference with customer relations, losses relating to a diminishment of Plaintiff's competitive standing in the market, loss of clients and business opportunities, loss of customer good will, and loss of business reputation.

Defendants maintain that they complied with the February 13, 2014 order because they performed searches of their electronic devices, including a term search for all 378 terms proposed by Castle, even though the request was unreasonable in light of their number and because the terms were so generic that they captured more "noise" than information. They point out that they did so before Plaintiff filed its second motion to compel, yet Castle's second motion to compel did not inform the Court that the forensic term search had already occurred.[10] Instead Castle alleged that Defendants did not comply with its discovery obligations because

[10] Castle finally admitted that the e-mail had been produced previously in its reply, #48-1.

they produced 148 documents after the February 2014 was issued and because Defendants' production showed that OSS misrepresented that it had no documents reflecting work performed by Byrne for OSS before he resigned from Castle. In an intentional or at best misguided attempt to mislead the Court, Castle cites a single e-mail dated March 7, 2013, subject: "Tenaris Contract Review for OSS PO 1001," to prove that Defendants had been withholding relevant documents. That email had first been produced by OSS on September 30, 2012, before Castle filed any motion to compel or before any Court order on discovery. The email was produced a second time on January 6, 2014, bates-labeled as OSS 00153, as part of the native files that had now been bates-labeled OSS_00001 through -000296, also prior to any motion to compel or Court order. The e-mail was produced again on July 23, 2014, as part of compliance with the February order, and Defendants' counsel specifically indicated that much of the production had been previously produced.[11] Thus the e-mail clearly did not support the relief Castle sought.

Defendants contend that they have been frustrated by Castle's refusal to identify what "confidential information" is involved

[11] In its reply, Castle concedes it did receive the three productions of this e-mail, but argues that the last had a different bates label and that Defendants did not identify the source as from the same electronic device nor did OSS's CEO Nick Jones acknowledge the existence of this email in his response to Castle's subpoena. It goes on to accuse Defendants of trying to hide the document and misrepresenting the nature of the communication. Its speculative charges are without any substantiating evidence.

here. When asked to identify specifically what documents Castle contended contained confidential information, Castle claimed virtually all of more than 10,000 pages produced by Defendants. #47-9, Castle's answer to Defendants' Second Set of Interrogatories.

Defendants insist that Castle has failed to produce any evidence of any default in Defendants' discovery responses, and highlight the fact that Magistrate Judge Stacy's February order found no default of discovery obligations or improper conduct by Defendants. As for her second order, Castle's deceptive reliance on the single email that had been produced three times, clearly not "new" evidence, does not prove that Byrne solicited business from Castle's customers before he resigned. Noting Castle's reliance on *Ameriwood Indus.,* 2006 WL 3825291, at *4, for the proposition that "discrepancies or inconsistencies in the responding party's discovery responses may justify a party's request to create and examine a mirror image of the hard drive," Defendants point out that the facts here differ from those in *Ameriwood Indus.*: no evidence has been produced that shows that OSS or Byrne failed to produce a document that has otherwise been shown to exist. Instead Castle's allegations are pure speculation and its repeated motions have become both an impermissible fishing expedition and harassment.

Although the September order compelled Castle to respond to

Defendants' discovery requests to identify employees given access to Castle's purported proprietary and confidential business information and evidence of damages it suffered as a result of lost business, goodwill, and reputation, limited to the oil and gas business unit where Byrne and other employees of OSS had worked, Castle failed to do so, but instead merely responded to each request, "Subject to and without waiving the foregoing general and specific objections, Castle states that its investigation continues." #57, Ex. A, Castle's supplemental responses to Defendants' First Request for Production.

Castle also objects that the Magistrate Judge failed to explain why she overruled Castle's objections and puts forth three reasons why Castle should not be required to comply with the September order: (1) when and why other employees left Castle is irrelevant to whether Defendants have been unfairly competing against Castle; (2) whether other employees had access to records taken by Defendants does not affect whether they consist of confidential information that Defendants should not have been using against Castle, nor does it relate to the merits of the claims Castle has asserted against them; and (3) the identity and complaints of other Castle customers who are not doing business with Byrne and OSS are not relevant to Castle's claims relating to customers that OSS has pursued using its information wrongfully obtained by Castle. Regarding (1), Defendants highlight Castle's

sworn response to an interrogatory that 10,343 of the 10,600 documents produced by Defendants (mainly thousands of e-mails dating back to 2006 on Leniek's non-Castle computer[12]) are Castle's "confidential information." Defendants emphasize that if Castle really intends to argue that they are all confidential information, Castle must prove that it acted to protect the secrecy of this kind of information with regard to other employees who left Castle's employment. As to (2), if information is widely shared and no measures are employed to restrict or limit access, the information cannot be confidential. Regarding (3), the identities and complaints of other Castle customers are relevant to Castle's claim for monetary damages, i.e., to issues raised in Castle's complaint about why customers have stopped doing business with Castle and how its reputation has been damaged. The Court fully concurs that Defendants' requests are highly relevant to the issues raised by Castle's pleadings.

In conclusion, Defendants urge the Court to overrule Castle's objections in their entirety for the reasons they give in their

[12] Defendants explain that Leniek worked as an independent contractor consultant for Castle and other companies in the oil and gas business and focused on South America. In order to increase its exposure in that area, Castle presumably gave Leniek the email address @amcastle.com so he could receive and send emails on behalf of Castle when he was working on non-Castle computers. Leniek received thousands of emails on his non-Castle computers. When Leniek's employment with Castle was terminated, Castle never sought to remove the emails from these computes, so when he received the subpoena from Castle, Leniek produced them in response.

response. Castle has failed to show that it is entitled to the forensic search it seeks, Defendants' motion to compel was reasonably tailored to obtain relevant, non-privileged information from Plaintiff to which it is entitled, and Castle has failed to show that Magistrate Judge Stacy's September 12, 2014 order was erroneous.

Castle's Reply (#51)

Castle's reply makes numerous speculative charges against Defendants of misrepresentation, concealment, and incompleteness of Defendants production of discovery without supporting evidence, reiterating some of its earlier challenges and trying to expand the scope of permissible discovery.

Court's Decision

Magistrate Judge Frances Stacy had broad discretion in reviewing the discovery challenges and she did not abuse that discretion. The Court finds that the Magistrate Judge's orders are not erroneous in fact or in law, but are thoughtful and tempered rulings that comply with the Federal Rules of Civil Procedure and the law regarding misappropriation of trade secrets and related claims. It agrees with Defendants that as the author, she is the best person to construe those orders and whether the parties complied with them, and she has done so convincingly.

Castle has failed to meet its burden to show that it is entitled to a court-supervised forensic inspection of Defendants'

computers and devices. "[A] party may not inspect the physical hard drives of a computer merely because the party wants to search for additional documents responsive to the party's document requests." *Ameriwood Indus.*, 2006 WL 382591, at *4, *citing McCurdy*, 9 Fed. Appx. at 831. The Court finds that Magistrate Judge Stacy did not err in finding that Defendants did not "default[] in [their] obligation to search [their records] and produce the requested data." *In re Weekley Homes*, 295 S.W. 3d at 317. Castle has not shown that Defendants are in wrongful possession of any company documents. They have not provided an expert's testimony, no less any other evidence, of their need to have the Court determine that Defendants were or have been deleting files. Meanwhile the Court agrees with Judge Stacy that Defendants have responded adequately to discovery requests and even hired an independent firm to perform a forensic examination to their computers that included a search for hundreds of terms requested by Castle. That Castle is skeptical, without anything else to support its request for an intrusive fishing expedition in Defendants electronic devices is insufficient to support such a drastic discovery request.

Furthermore, for purposes of its objections and request for such a search, Castle has not even met its burden to establish that it had trade secrets, while Defendants have raised substantial questions whether trade secrets existed in this dispute (e.g.,

whether the alleged materials were secret, whether Byrne acquired them by improper means, whether other employees and ex-employees knew about them and considered them to be confidential, and whether Castle took adequate measures to keep them secret).

Accordingly, the Court

ORDERS that Castle's objections (#53) are OVERRULED.

SIGNED at Houston, Texas, this 12th day of August, 2015.

MELINDA HARMON
UNITED STATES DISTRICT JUDGE